lifetime of the master secret. Once the master secret lifetime has expired, the first and second computer system would then securely renegotiate another master secret.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by United States Letters Patent is:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

1. In a network system that includes a first computer system network connectable to a second computer system, the first computer system capable of encrypting data, a method of the first computer system encrypting data so as to guard against eavesdropping and brute force attacks, the method comprising the following:

an act of securely negotiating a master secret with the second computer system;

an act of generating a random bit sequence;

an act of including the random bit sequence in a seed to generate a random seed;

an act of inputting the master secret and the random seed into a key generation module to generate a key;

an act of using the key to encrypt data; and

an act of including the encrypted data and the random seed in a data structure.

2. A method in accordance with Claim 1, wherein the data structure is a data packet, the method further comprising an act of transmitting the data packet in accordance with a protocol.

3. A method in accordance with Claim 2, wherein the data packet includes a Security Parameter Index in accordance with the Encapsulating Security Payload (ESP) protocol.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

4. A method in accordance with Claim 2, wherein the acts of generating a random bit sequence, including the random bit sequence in a seed, inputting the master secret and the random seed, using a key to encrypt data, including the encrypted data and the random seed in a data structure, and transmitting the data packet are performed for each of a plurality of data packets, wherein the random number is randomly generated for each data packet.

5. A method in accordance with Claim 2, wherein the protocol comprises an unconfirmed push protocol.

6. A method in accordance with Claim 5, wherein the unconfirmed push protocol comprises User Datagram Protocol (UDP).

7. A method in accordance with Claim 1, further comprising an act of negotiating a parameter expiry with the second computer system, the parameter expiry indicating the lifetime of the master secret.

8. A method in accordance with Claim 7, wherein upon expiration of the lifetime of the master secret, performing an act securely renegotiating a master secret with the second computer system.

9. A method in accordance with Claim 1, wherein the second computer system comprises a wireless device.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

10. A method in accordance with Claim 1, wherein the act of generating a random bit sequence is performed by a cryptographically secure random number generator.

11. A method in accordance with Claim 1, further comprising an act of including, in the random seed, a bit sequence that represents the current time.

12. A method in accordance with Claim 1, wherein the random seed is at least 96 bits.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

13. A computer program product for use in a network system that includes a first computer system network connectable to a second computer system, the computer program product for implementing a method of the first computer system encrypting data so as to guard against eavesdropping and brute force attacks, the computer program product comprising a computer-readable medium having stored thereon the following:

computer-executable instructions for performing an act of securely negotiating a master secret with the second computer system;

computer-executable instructions for performing an act of generating a random bit sequence;

computer-executable instructions for performing an act of including the random bit sequence in a seed to generate a random seed;

computer-executable instructions for performing an act of inputting the master secret and the random seed into a key generation module to generate a key;

computer-executable instructions for performing an act of using the key to encrypt data; and

computer-executable instructions for performing an act of including the encrypted data and the random seed in a data structure.

14. The computer program product as recited in Claim 13, wherein the computer-readable medium is a physical storage medium.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

15. In a network system that includes a first computer system network connectable to a second computer system, the first computer system capable of encrypting data, a method of the first computer system encrypting data so as to guard against eavesdropping and brute force attacks, the method comprising the following:

an act of securely negotiating a master secret with the second computer system;

a step for generating a key using the master secret and the random seed so that the master secret and key are difficult for an eavesdropper to identify;

an act of using the key to encrypt data; and

an act of including the encrypted data and the random seed in a data structure.

16. A method in accordance with Claim 15, wherein the data structure is a data packet, the method further comprising an act of transmitting the data packet in accordance with a protocol to the second computer system.

17. A method in accordance with Claim 16, wherein the step for generating a key, the act of using the key to encrypt data, the act of including the encrypted data and random seed in a data structure, and the act of transmitting the data packet are performed for each of a plurality of data packets, wherein the random number is randomly generated for each data packet.

18. A method in accordance with Claim 16, wherein the protocol comprises an unconfirmed push protocol.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

19. A method in accordance with Claim 18, wherein the unconfirmed push protocol comprises User Datagram Protocol (UDP).

20. A method in accordance with Claim 15, wherein the second computer system comprises a wireless device.

21. A method in accordance with Claim 15, further comprising an act of including, in the random seed, a bit sequence that represents the current time.

22. A method in accordance with Claim 15, wherein the step for generating a key using the master secret and the random seed comprises the following:

an act of generating a random bit sequence;

an act of including the random bit sequence in a seed to generate the random seed; and

an act of inputting the master secret and the random seed into a key generation module to generate a key.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

23. In a network system that includes a first computer system network connectable to a second computer system, a method of the second computer system decrypting a data packet that was transmitted to the second computer system by the first computer system, the data packet being encrypted so as to guard against eavesdropping and brute force attacks, the method comprising the following:

an act of securely negotiating a master secret with the first computer system;

an act of receiving a data packet from the first computer system;

an act of reading a random seed from the data packet received from the first computer system, the random seed including a random bit sequence generated by a random number generator;

an act of inputting the master secret and the random seed into a key generation module to generate a key; and

an act of using the key to decrypt the data packet.

24. A method in accordance with Claim 23, wherein the data packet includes a Security Parameter Index in accordance with the Encapsulating Security Payload (ESP) protocol.

25. A method in accordance with Claim 23, wherein the acts of receiving a data packet, reading a random seed from the data packet, inputting the master secret and the random seed into a key generation module to generate a key, and using the key to decrypt the data packet are performed for each of a plurality of data packets, wherein the random seed includes a different random bit sequence for each data packet.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

26. A method in accordance with Claim 23, wherein the data packet is received using an unconfirmed push protocol.

27. A method in accordance with Claim 26, wherein the unconfirmed push protocol comprises User Datagram Protocol (UDP).

28. A method in accordance with Claim 23, further comprising an act of negotiating a parameter expiry with the first computer system, the parameter expiry indicating the lifetime of the master secret.

29. A method in accordance with Claim 28, wherein upon expiration of the lifetime of the master secret, performing an act securely renegotiating a master secret with the first computer system.

30. A method in accordance with Claim 29, wherein the second computer system comprises a wireless device.

31. A method in accordance with Claim 23, wherein the random seed includes a bit sequence that represents the current time.

32. A method in accordance with Claim 23, wherein the random seed is at least 96 bits.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111
TEL: (801) 533-9800

33. A computer program product for use in a network system that includes a first computer system network connectable to a second computer system, the computer program product for implementing a method of the second computer system decrypting a data packet that was transmitted to the second computer system by the first computer system, the data packet being encrypted so as to guard against eavesdropping and brute force attacks, the computer program product comprising a computer-readable medium having stored thereon the following:

computer-executable instructions for performing an act of securely negotiating a master secret with the first computer system;

computer-executable instructions for performing an act of detecting the receipt of a data packet from the first computer system;

computer-executable instructions for performing an act of reading a random seed from the data packet received from the first computer system, the random seed including a random bit sequence generated by a random number generator;

computer-executable instructions for performing an act of inputting the master secret and the random seed into a key generation module to generate a key; and

computer-executable instructions for performing an act of using the key to decrypt the data packet.

34. A computer program product in accordance with Claim 33, wherein the computer-readable medium is a physical storage medium.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

35. In a network system comprising a plurality of server computer system connectable through a network with a plurality of client computer systems, the network system comprising the following:

a server computer system configured to securely negotiate a master secret with a client computer system, generate and include a random bit sequence in a seed to generate a random seed, input the master secret and the random seed into a server-side key generation module to generate a key, use the key to encrypt a data packet, and transmit the data packet to the client computer system; and

the client computer system, the client computer system further configured to receive the data packet from the server computer system, read the random seed from the data packet, input the master secret and the random seed into a client side key generation module to generate a key, and decrypt the data packet.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111
TEL FAX